## AMENDMENT TO THE CLAIMS

1. (Currently Amended) A cryptographic method, including:

generating, at a first entity, a first public key $M_B$, the first public key $M_B$ being session specific;

receiving from a second entity, at the first entity, a second public key $M_A$, the second public key $M_A$ being session specific;

generating, at the first entity, a first secret $S_B$ by hashing one or more parameters that are known to the first entity and the second entity, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, the first public key $M_B$, and the second public key $M_A$;

generating, at the first entity, a first session key $K_B$, the first session key $K_B$ being different from the first secret $S_B$, both the first session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

encrypting, at the first entity, a first random nonce $N_B$ with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting, at the first entity, the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first entity to the second entity;

receiving a response to the encrypted random nonce; and

authenticating through determining whether the response includes a correct modification of the first random nonce $N_B$.

2. (Canceled)

3. (Previously Presented) The method of claim 1 wherein authenticating through determining whether the response includes a correct modification includes:

checking whether a received modification of the first random nonce $N_B$ equals a modification of the first random nonce $N_B$ applied by the first entity.

4. (Previously Presented) The method of claim 1 wherein said authenticating includes:
checking whether a received modification of the first random nonce less a modification thereof as applied thereto by the first entity equals the first random nonce.

5. (Previously Presented) The method of claim 1 wherein generating the first session key $K_B$ includes:
generating a first random number $R_B$, and
computing the first session key $K_B$ from the second public key $M_A$ raised to the exponential power of the first random number $R_B$, modulo a parameter $ß_B$.

6-7. (Canceled)

8. (Previously Presented) The method of claim 1 wherein said generating the first secret $S_B$ includes:
combining the second public key $M_A$ and the first public key $M_B$ with a first password $P_B$ to produce a first result, and
hashing the first result with a secure hash.

9. (Original) The method of claim 8 wherein the secure hash is a one-way hash function.

10. (Original) The method of claim 9 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvennyl Standard.

11. (Previously Presented) The method of claim 1 wherein said generating the first secret $S_B$ includes:
combining a first password $P_B$ and at least one of the second public key $M_A$ and the first public key $M_B$ to generate a first combined result, and
combining the first combined result and at least one of the second public key $M_A$, the first password $P_B$, and the first public key $M_B$ to generate a second combined result.

12. (Previously Presented) The method of claim 1 wherein the first random nonce $N_B$ is encrypted using a symmetrical encryption algorithm.

13. (Original) The method of claim 12, wherein the symmetrical encryption algorithm is one of the Data Encryption Standard and the block cipher CAST.

14. (Previously Presented) The method of claim 1 wherein encrypting the first random nonce $N_B$ includes superencrypting the first random nonce $N_B$.

15. (Previously Presented) The method of claim 14, wherein superencrypting the first random nonce $N_B$ includes:
encrypting the first random nonce $N_B$ with the first secret $S_B$ to produce the first encrypted result; and
encrypting the first encrypted result using the first session key $K_B$.

16. (Previously Presented) The method of claim 15 wherein said authenticating includes:
decrypting the response using the first session key $K_B$ to generate a first decrypted result; and
decrypting the first decrypted result using the first secret $S_B$.

17. (Previously Presented) The method of claim 1, wherein the response includes a combination of a second random nonce $N_A$ and a modification of the first random nonce; and wherein the method further includes:
extracting the second random nonce $N_A$ from the response;
modifying the second random nonce $N_A$ to obtain a modified second random nonce;
encrypting the modified second random nonce using the first session key $K_B$ and the first secret $S_B$ to obtain an encrypted package; and
transmitting the encrypted package from the first entity.

18. (Previously Presented) The method of claim 17 wherein said encrypting the modified second random nonce includes:

generating a string of random bits $I_B$;

encrypting a combination of the string of random bits $I_B$ and the modified second random nonce using the first secret $S_B$ to generate a first result; and

encrypting the first result using the first session key $K_B$.

19. (Previously Presented) The method of claim 17 wherein the encrypted package is transmitted for authentication of the first entity in opening a two-way communication channel.

20. (Currently Amended) A computer readable storage medium containing executable computer program instructions which, when executed, cause a first computer system to perform a cryptographic method including:

generating, at the first computer system, a first public key $M_B$, the first public key $M_B$ being session specific;

receiving from a second computer system, at the first computer system, a second public key $M_A$, the second public key $M_A$ being session specific;

generating, at the first computer system, a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~ one or more of the following: a first password $P_B$, the first public key $M_B$, and the second public key $M_A$;

generating, at the first computer system, a first session key $K_B$, the first session key $K_B$ being different from the first secret $S_B$, both the first session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

encrypting, at the first computer system, a first random nonce $N_B$ with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting, at the first computer system, the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random nonce;

transmitting the encrypted random nonce from the first computer system to the second computer system; and

authenticating through determining whether a response to the encrypted random nonce includes a correct modification of the first random nonce $N_B$.

21. (Currently Amended) A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a computer cryptographic method through a network, the method comprising:

generating at the first computer system a first public key $M_B$, the first public key $M_B$ being session specific;

generating at the second computer system a second public key $M_A$, the second public key $M_A$ being session specific;

receiving at the first computer system the second public key $M_A$;

generating, at the first computer system, a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, the first public key $M_B$, and the second public key $M_A$;

generating at the first computer system a session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

generating at the first computer system a first random nonce $N_B$;

encrypting at the first computer system the first random nonce $N_B$ with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting at the first computer system the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random nonce;

transmitting the encrypted random nonce and the first public key $M_B$ from the first computer system to the second computer system to establish the session key at the second computer system;

receiving at the first computer system from the second computer system a response to the encrypted random nonce; and

authenticating the second computer system at the first computer system through determining whether the response includes a correct modification of the first random nonce $N_B$.

22. (Currently Amended) A computer system for performing a cryptographic method through a network, the computer system comprising:

a processor;

a network interface coupled to the network and coupled to the processor, the network interface to receive a request including information on a user identification; and

a storage device coupled to the processor, the storage device to store a user password corresponding to the user identification, and wherein the processor is to perform a method, including:

receiving a second public key $M_A$ through the network interface from a second computer system, the second public key $M_A$ being session specific;

generating, at the first computer system, a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, the first public key $M_B$, and the second public key $M_A$;

generating a first session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

generating a first public key $M_B$, the first public key $M_B$ being session specific;

generating a first random nonce $N_B$, the first random nonce $N_{BB}$;

encrypting the first random nonce $N_B$ with the session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting the first encrypted result with the other one of the session key $K_B$ or the first secret $S_B$ to obtain an encrypted random nonce;

transmitting the encrypted random nonce and the first public key $M_B$ through the network interface;

authenticating through determining whether a response to the encrypted random nonce includes a correct modification of the first random nonce.

23. (Previously Presented) The computer system of claim 22 wherein the network is a network operating according to a hypertext transfer protocol; and the first public key $M_B$ is transmitted with the encrypted random nonce for session key exchange.

24. (Currently Amended) A cryptographic method, comprising:

receiving at a first entity a second public key $M_A$ and an encrypted second random number from a second entity;

generating a first secret $S_B$ by hashing one or more parameters that are known to the first entity and the second entity, at least one of the parameters being a result of hashing ~~equal to a sequence of has functions applied to at least~~one or more of the following: a first password $P_B$, a first public key $M_B$, and the second public key $M_A$;

generating a first session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

decrypting, using the first secret $S_B$ and the first session key $K_B$, to retrieve a second random number $N_A$ from the encrypted second random number;

modifying the second random number $N_A$ to obtain a modified second random number;

encrypting the modified second random number with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random package; and

transmitting the encrypted random package from the first entity.

25. (Previously Presented) The method of claim 24, wherein said decrypting includes:

decrypting the encrypted second random number using the first session key $K_B$ to generate the first decrypted result; and

decrypting the first decrypted result using at least a first password $P_B$ and the second public key $M_A$.

26. (Previously Presented) The method of claim 24 wherein said generating the first session key $K_B$ includes:

generating a first random number $R_B$, and

computing the first session key $K_B$ from the second public key $M_A$ raised to the exponential power of the first random number $R_B$, modulo a parameter $ß_B$.

27-28. (Canceled)

29. (Previously Presented) The method of claim 24 wherein said generating the first secret $S_B$ includes:

combining the first public key $M_B$ with the first password $P_B$ to produce a first result, and

hashing the first result with a secure hash.

30. (Original) The method of claim 29 wherein the secure hash is a one-way hash function.

31. (Original) The method of claim 30 wherein the one-way hash function is one of the Secure Hash Algorithm, the Message Digest 5, Snefru, Nippon Telephone and Telegraph Hash, and the Gosudarstvennyl Standard.

32. (Previously Presented) The method of claim 24 wherein said generating the first secret $S_B$ includes:

combining the first password $P_B$ and the first public key $M_B$ to generate a first combined result, and

combining the first combined result and at least one of the second public key $M_A$, the first password $P_B$, and the first public key $M_B$ to generate the first secret $S_B$.

33. (Previously Presented) The method of claim 24, wherein said encrypting the modified second random number includes superencrypting the modified second random number.

34. (Previously Presented) The method of claim 24, further including:
generating a first random number $N_B$; and
wherein said encrypting the modified second random number includes:
encrypting a combination of the first random number $N_B$ and the modified second random number.

35. (Previously Presented) The method of claim 34 which further includes:
receiving at the first entity a response to the encrypted random package;
decrypting the response to obtain a combination of a string of random bits and a modified first random nonce; and
retrieving the modified first random nonce from the combination of the string of random bits and the modified first random nonce;
determining whether the modified first random nonce was correctly modified from the first random number $N_B$.

36. (Previously Presented) The method of claim 35 wherein said determining whether the modified first random nonce was correctly modified includes:
checking whether the modified first random nonce equals a modification of the first random nonce as applied to the first random nonce by the first entity.

37. (Previously Presented) The method of claim 35 wherein said determining whether the modified first random nonce was correctly modified includes:
checking whether the modified first random nonce less a modification thereof as applied thereto by the first entity equals the first random nonce.

38. (Currently Amended) A computer readable storage medium containing executable computer program instructions which, when executed, cause a first computer system to perform a cryptographic method including:

receiving at the first computer system a second public key $M_A$ and an encrypted second random number from a second computer system;

generating a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, a first public key $M_B$, and the second public key $M_A$;

generating a first session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

decrypting, using the first secret $S_B$ and the first session key $K_B$, to retrieve the second random number $N_A$ from the encrypted second random number;

modifying the second random number $N_A$ to obtain a modified second random number;

encrypting the modified second random number with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system for authentication.

39. (Currently Amended) A distributed readable storage medium containing executable computer program instructions which, when executed, cause a first computer system and a second computer system to perform a cryptographic method through a network, the method including:

receiving, from the second computer system and at the first computer system, a second public key $M_A$ and an encrypted second random number;

generating a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, a first public key $M_B$, and the second public key $M_A$;

generating a first session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

decrypting, using the first secret $S_B$, to retrieve a second random number $N_A$ from the encrypted second random number;

modifying the second random number $N_A$ to obtain a modified second random number;

encrypting the modified second random number with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random package;

transmitting the encrypted random package from the first computer system to the second computer system.

40. (Currently Amended) A computer system for performing a cryptographic method through a network, the computer system comprising:

a processor;

a network interface coupled to the network and coupled to the processor, the network interface to receive a request including information on a user identification; and

a storage device coupled to the processor, the storage device to store a user password associated with the user identification, and wherein the processor is to perform a method, including

generating a first public key $M_B$;

receiving a second public key $M_A$ and an encrypted second random number through the network interface from a second computer system;

generating a first secret $S_B$ by hashing one or more parameters that are known to the first computer system and the second computer system, at least one of the parameters being a result of hashing ~~equal to a sequence of hash functions applied to at least~~one or more of the following: a first password $P_B$, a first public key $M_B$, and the second public key $M_A$;

generating a first session key $K_B$, the session key $K_B$ being different from the first secret $S_B$, both the session key $K_B$ and the first secret $S_B$ being computed from the second public key $M_A$;

decrypting, using the first secret $S_B$ and the first session key $K_B$, to retrieve the second random number $N_A$ from the encrypted second random number;

modifying the second random number $N_A$ to obtain a modified second random number;

encrypting the modified second random number with the first session key $K_B$ or the first secret $S_B$ to obtain a first encrypted result;

encrypting the first encrypted result with the other one of the first session key $K_B$ or the first secret $S_B$ to obtain an encrypted random package;

transmitting the encrypted random package through the network interface.

41. (Previously Presented) The computer system of claim 40 wherein the network is a network operating according to a hypertext transfer protocol; and the first public key $M_B$ is transmitted for session key exchange before the encrypted second random number is received.